

IN THE UNITED STATES DISTRICT COURT  
DISTRICT OF OREGON

AL-HARAMAIN ISLAMIC FOUNDATION, INC., an Oregon Nonprofit Corporation, WENDELL BELEW, a U.S. Citizen and Attorney at Law, ASIM GHAFOOR, a U.S. Citizen and Attorney at Law,	)	
	)	
Plaintiffs,	)	Case No. 06-274-KI
	)	
vs.	)	OPINION AND ORDER
	)	
GEORGE W. BUSH, President of the United States, NATIONAL SECURITY AGENCY, KEITH B. ALEXANDER, its Director, OFFICE OF FOREIGN ASSETS CONTROL, an office of the United States Treasury, ROBERT W. WERNER, its Director, FEDERAL BUREAU OF INVESTIGATION, ROBERT S. MUELLER, III, its Director,	)	
	)	
Defendants,	)	
	)	
and	)	
	)	

OREGON PUBLISHING COMPANY, )  
 )  
 Intervenor. )  
 \_\_\_\_\_ )

Jon B. Eisenberg  
Attorney at Law  
1970 Broadway, Suite 1200  
Oakland, California 94612

Lisa R. Jaskol  
Attorney at Law  
15760 Ventura Boulevard, 18th Floor  
Encino, California 91436

Steven Goldberg  
American Bank Building  
621 S. W. Morrison, Suite 1450  
Portland, Oregon 97205

Thomas H. Nelson  
Zaha S. Hassan  
Thomas H. Nelson & Associates  
825 N.E. Multnomah, Suite 925  
Portland, Oregon 97232

Jessica Ashlee Albies  
Law Office of J. Ashlee Albies  
621 S.W. Alder Street, Suite 621  
Portland, Oregon 97205

Attorneys for Plaintiffs

Andrea Marie Gacki  
U.S. Department of Justice  
Civil Division / Federal Programs Branch  
20 Massachusetts Avenue, N.W., Room 7334  
Washington, D.C. 20001

Andrew H. Tannenbaum  
U.S. Department of Justice  
20 Massachusetts Avenue, N.W.  
P. O. Box 883  
Washington, D.C. 20044

Anthony J. Coppolino  
U.S. Department of Justice  
20 Massachusetts Avenue, N.W., Room 6102  
Washington, D.C. 20530

Attorneys for Defendants

Charles F. Hinkle  
Emilie K. Edling  
Stoel Rives, LLP  
900 SW Fifth Avenue, Suite 2600  
Portland, Oregon 97204

Attorneys for Intervenor

KING, Judge:

Plaintiffs Al-Haramain Islamic Foundation, Inc., Wendell Belew, and Asim Ghafoor filed suit against George W. Bush, the National Security Agency (“NSA”), the Office of Foreign Assets Control (“OFAC”), the Federal Bureau of Investigation (“FBI”), and the respective agency directors (collectively, “the government”) for violations of the Foreign Intelligence Surveillance Act (“FISA”), the Separation of Powers clause, the Fourth, First and Sixth Amendments to the United States Constitution, and the International Convention for the Suppression of the Financing of Terrorism. The government has filed a Motion to Dismiss or, in the Alternative, for Summary Judgment (#58) and a Motion to Prevent Plaintiffs’ Access to the Sealed Classified Document (#39). Plaintiffs have filed a Motion for Order Compelling Discovery (#35). Oregonian Publishing Company has filed a Motion to Intervene and to Unseal Records (#7).

For the reasons described herein, the government’s Motion to Dismiss is denied, and its Motion for Summary Judgment is denied with leave to renew. The government’s Motion to Prevent Plaintiffs’ Access to the Sealed Classified Document is granted. Plaintiffs’ Motion for

Order Compelling Discovery is denied with leave to renew. Oregonian Publishing Company's Motion to Intervene was previously granted on April 25, 2006, and its Motion to Unseal Records is denied.

## **BACKGROUND**

### I. Factual Background

On December 17, 2005, in a radio address, and in response to an article the day before in *The New York Times*, President George W. Bush announced that he had authorized "the interception of international communications of people with known links to al Qaeda and related terrorist organizations" ("Surveillance Program") after the September 11, 2001 attacks.<sup>1</sup> President's Radio Address (Dec. 17, 2005), *available at* <http://www.whitehouse.gov//news/releases/2005/12/20051217.html>. Attorney General Alberto Gonzalez subsequently confirmed that the Surveillance Program intercepts communications where one party to the communication is outside the United States and the government has a reasonable basis to believe that at least one party to the communication is affiliated with, or working in support of, al Qaeda.

Plaintiffs allege in their Complaint that in February 2004 OFAC froze Al-Haramain's assets while investigating whether Al-Haramain was engaged in terrorist activities. At that time, Al-Haramain was affiliated with and supported by Al-Haramain Islamic Foundation, a charity in Saudi Arabia. Plaintiffs allege that Al-Haramain's assets were frozen as a result of warrantless electronic surveillance between a director or directors of Al-Haramain and its attorneys, Belew

---

<sup>1</sup>The government refers to the program as the "Terrorist Surveillance Program" or "TSP" in its briefing, while plaintiffs refer to the program as the "warrantless surveillance program."

and Ghafoor. Plaintiffs also allege that in March and April 2004 the NSA engaged in electronic surveillance of communications between Al-Haramain's director or directors and Belew and Ghafoor, without obtaining a court order or otherwise following the procedures required under FISA. They further allege that in May 2004, the NSA turned over logs of these conversations to OFAC, which subsequently identified Al-Haramain as a "specially designated global terrorist" in September 2004.

The government offers some additional information about Al-Haramain. It explains that the identification of Al-Haramain as a specially designated global terrorist was due to its having provided support to al Qaeda, Osama bin Laden, and other specially designated global terrorists. In addition, the United Nations Security Council has identified Al-Haramain as an entity belonging to or associated with al Qaeda. The government also explains that Soliman Al-Buthi,<sup>2</sup> a director of Al-Haramain and a citizen of Saudi Arabia, has been identified as a specially designated global terrorist.

Plaintiffs seek a declaration that the surveillance of them was unlawful, seek disclosure of the communications, information, and records obtained as a result of the surveillance, along with the subsequent destruction of such information and records, seek to enjoin warrantless surveillance of plaintiffs, seek \$1,000 or \$100 per day for each violation of FISA, and seek punitive damages of \$1,000,000, costs and attorney fees.

Along with their Complaint, plaintiffs filed a document under seal with the Court (the "Sealed Document"). OFAC inadvertently disclosed this document to counsel for Al-Haramain

---

<sup>2</sup>The government spells this individual's name as Al'Buthe, but I will employ plaintiffs' spelling.

in late August 2004 as part of a production of unclassified documents relating to Al-Haramain's potential status as a specially designated global terrorist.

Lynne Bernabei, an attorney for Al-Haramain and for two of its directors, Al-Buthi and Pirouz Sedaghaty (a k a Pete Seda), testified in a declaration about the circumstances surrounding her dissemination of the Sealed Document. Upon receiving the packet of materials from OFAC, she copied and disseminated the materials, including the pertinent document which was labeled "TOP SECRET," to Al-Haramain's directors and Bernabei's co-counsel. In August or September, a reporter from the Washington Post reviewed these documents for an article he was researching. On October 7, 2004, Bernabei learned from the FBI that included among the produced documents was a sensitive document that OFAC claimed had been inadvertently released. At the request of the FBI, Bernabei and her co-counsel returned their copies of the sensitive document to the FBI. The FBI did not pursue Al-Haramain's directors, whom the government describes as "likely recipients" of the document, to ask them to return their copies.

The government asserts that the Sealed Document carries a classification of "TOP SECRET" and that it contains "sensitive compartmented information" or "SCI." The Sealed Document is now in the Secure Compartmentalized Information Facility at the FBI office in Portland ("SCIF").

## II. Procedural Background

On March 17, 2006, the Oregonian Publishing Company filed a Motion to Intervene and to Unseal Records. On May 22, 2006, plaintiffs filed a Motion for Order Compelling Discovery, seeking to compel the government to respond to interrogatories requesting information about electronic surveillance of the plaintiffs and information regarding the reasons for classifying the

Sealed Document. On May 26, 2006, the government filed a Motion to Prevent Plaintiffs' Access to the Sealed Classified Document.

On June 21, 2006, the government filed a Motion to Dismiss or, in the Alternative, for Summary Judgment. In this motion, the government asserts the military and state secrets privilege ("state secrets privilege"), arguing that the case should be dismissed or, in the alternative, that summary judgment should be granted in favor of the government based on the privilege. In support of its assertion of the privilege, the government provided unclassified declarations of John D. Negroponte, Director of National Intelligence, and Lieutenant General Keith B. Alexander, Director, National Security Agency. In addition, the government lodged classified materials for *in camera, ex parte* review. Specifically, the government submitted classified declarations of Negroponte and Alexander, as well as classified versions of its memorandum and reply in support of its motion to dismiss, and its opposition to plaintiffs' motion to compel. Plaintiffs objected to the lodging of the materials for *in camera, ex parte* review.

In order to better prepare myself for oral argument, and to assess the government's assertion of the state secrets privilege, I ruled on August 18, 2006 that I would review the government's *in camera, ex parte* materials filed with the Court on June 21, 2006 and July 25, 2006. The Ninth Circuit has noted that it is "unexceptionable" for the government to elaborate on public filings with *in camera* submissions and for judges to review such filings to determine the validity of the claim of privilege. Kasza v. Browner, 133 F.3d 1159, 1169 (9<sup>th</sup> Cir. 1998) (collecting cases); see also United States v. Ott, 827 F.2d 473, 476-77 (9<sup>th</sup> Cir. 1987) (*ex parte, in camera* review of FISA material does not deprive a defendant of due process). The D.C. Circuit

has noted that it is also “well settled” that evaluation of the legitimacy of a state secrets privilege claim should not involve the participation of plaintiff’s counsel in the *in camera* examination of putatively privileged material. Ellsberg v. Mitchell, 709 F.2d 51, 61 (D.C. Cir. 1983) (describing district court and court of appeals inspection of *in camera* submissions). However, since the government had not yet asserted the state secrets privilege at the time of filing the *in camera, ex parte* declarations on April 14, 2006 and May 12, 2006, supporting its opposition to the Oregonian’s motion, I declined to review those submissions.

## **DISCUSSION**

### I. The State Secrets Privilege

The government’s assertion of the state secrets privilege is the threshold issue in this case. According to the government, its invocation of the privilege requires that plaintiffs’ case be dismissed for several alternative reasons, that it supports the government’s motion to prevent plaintiffs’ access to the Sealed Document, and that it justifies the denial of the plaintiffs’ motion for an order compelling discovery.

The state secrets privilege is a common law evidentiary privilege that allows the government to deny discovery of military and state secrets. United States v. Reynolds, 345 U.S. 1, 7-8 (1953); Kasza, 133 F.3d at 1165. Once the government properly invokes the privilege, the court’s task is to determine whether there is a reasonable danger that national security would be harmed by the disclosure of state secrets. Kasza, 133 F.3d at 1166. Once the court is so satisfied, the privilege is absolute. Id.

The state secrets privilege does not allow a balancing of necessity to the party seeking disclosure against potential harm from disclosure. Reynolds, 345 U.S. at 11; Kasza, 133 F.3d at

1166. Indeed, the court must treat the invocation of the privilege with the “utmost deference” and apply a “narrow” scope of review when evaluating the claim. Kasza, 133 F.3d at 1166. However, the Supreme Court in Reynolds noted that where there is a strong showing of necessity, the assertion of privilege should not be “lightly accepted.” Reynolds, 345 U.S. at 11.

The state secrets privilege may require dismissal of a case for any of three reasons: (1) if specific evidence must be removed from the case as privileged, but plaintiff can no longer prove the *prima facie* elements of the claim without that evidence; (2) if the defendant is unable to assert a valid defense without evidence covered by the privilege; (3) even if the plaintiff is able to produce nonprivileged evidence, the “very subject matter of the action” is a state secret. Kasza, 133 F.3d at 1166.

Courts have characterized outright dismissal of a suit based on the state secrets privilege as a “drastic” and “draconian” remedy. In re United States, 872 F.2d 472, 477 (D.C. Cir. 1989); Fitzgerald v. Penthouse Int’l, Ltd., 776 F.2d 1236, 1242 (4<sup>th</sup> Cir. 1985). Indeed, one court has noted that “whenever possible, sensitive information must be disentangled from nonsensitive information to allow for the release of the latter.” Ellsberg, 709 F.2d at 57. However, courts have recognized that there are inherent limitations in trying to separate classified and unclassified information, comparing contemporary electronic intelligence gathering to the construction of a “mosaic,” from which pieces of “seemingly innocuous information” can be analyzed and cobbled together to reveal the full operational picture. Kasza, 133 F.3d at 1166 (quoting Halkin v. Helms, 598 F.2d 1, 8 (D.C. Cir. 1978)).

In attempting to limit the application of the state secrets privilege and allow cases to proceed despite the absence of some privileged information, courts have endorsed the item-by-

item *in camera* review of evidence to determine which evidence was properly subject to the state secrets privilege, or have encouraged other procedural innovations to allow trials to proceed while limiting disclosure of information covered by the privilege. See e.g., In re United States, 872 F.2d at 479 (item-by-item *in camera* review of evidence for privilege was within the district court's discretion); Ellsberg, 709 F.2d at 64 (recognizing that the trial judge had discretion to develop procedural innovations to ensure that the government justifies its privilege); Hepting v. AT&T Corp., No. C-06-672 VRW, 2006 WL 2038464, at \* 34 (N.D. Cal. July 20, 2006) (requesting guidance from the parties on how best to carry out the court's duty to disentangle sensitive information from non-sensitive information, including a proposal to appoint a special master to consider classified evidence).

A. Procedural Invocation of the Privilege

The parties do not dispute that the government followed the proper steps to invoke the privilege when the heads of the responsible departments lodged a formal claim of privilege. See Reynolds, 345 U.S. at 7.

B. Plaintiffs' Showing of Necessity for the Information

I must next determine whether plaintiffs have demonstrated a strong showing of necessity for the information over which the government claims the privilege. Reynolds, 345 U.S. at 11. While plaintiffs expressly state that they have no need to learn any secret information about the nature and severity of the al Qaeda threat, or about the means and methods of the Surveillance Program, they have asserted a need for information contained in the Sealed Document. According to plaintiffs, the document shows that their communications were intercepted under the Surveillance Program, demonstrating their standing to sue, and "bolstering . . . the inference

that defendants had the requisite intent for a FISA violation.” Pls.’ Mem. in Opp’n to Defs.’ Mot. to Dismiss at 15. Accordingly, plaintiffs need some information in the Sealed Document to establish their standing and a *prima facie* case, and they have no other available source for this information. See Reynolds, 345 U.S. at 11. As a result, I cannot “lightly accept” the government’s claim of privilege. Id.

C. What Information is Secret

The government lists four categories of information that it says are implicated by this case, and that it contends must be protected from disclosure: (i) information regarding the al Qaeda threat, (ii) information regarding the Surveillance Program; (iii) information that would confirm or deny whether plaintiffs have been subject to surveillance under the Surveillance Program or under any other government program; and (iv) information pertaining to the Sealed Document.

Prior to determining whether the state secrets privilege requires dismissal of plaintiff’s case, I first determine whether this information qualifies as a secret. Hepting, 2006 WL 2038464, \* 9; El-Masri v. Tenet, 437 F. Supp. 2d 530, 536 (E.D. Va. 2006), American Civil Liberties Union v. Nat’l Security Agency, 06-CV-10204, 2006 WL 2371463, at \*7 (E.D. Mich., August 17, 2006).

\_\_\_\_\_  
Taking the second category of information first, I summarize what has been publicly disclosed by official sources about the Surveillance Program. President George W. Bush announced in a radio address that he had authorized the NSA to begin a program to intercept international communications of people with known links to al Qaeda and related terrorist organizations. He explained generally how it works:

The activities I authorized are reviewed approximately every 45 days. Each review is based on a fresh intelligence assessment of terrorist threats to the continuity of our government and the threat of catastrophic damage to our homeland. During each assessment, previous activities under the authorization are reviewed. The review includes approval by our nation's top legal officials, including the Attorney General and the Counsel to the President. I have reauthorized this program more than 30 times since the September the 11<sup>th</sup> attacks, and I intend to do so for as long as our nation faces a continuing threat from al Qaeda and related groups.

President's Radio Address (Dec. 17, 2005), *available at*

<http://www.whitehouse.gov//news/releases/2005/12/20051217.html>. It is clear from this description that the government does not seek a warrant prior to intercepting communications under the Surveillance Program.

Two days later, Attorney General Alberto Gonzalez verified that the Surveillance Program intercepts communications where one party to the communication is outside the United States and the government has "a reasonable basis to conclude that one party to the communication is a member of al Qaeda, affiliated with al Qaeda, or a member of an organization affiliated with al Qaeda, or working in support of al Qaeda." Press Briefing by Attorney General Alberto Gonzales and General Michael Hayden, Principal Deputy Director for National Intelligence (Dec. 19, 2005), *available at*

<http://www.whitehouse.gov//news/releases/2005/12/20051219-1.html>.

In addition, the United States Department of Justice issued a 42-page white paper explaining its legal theories in support of the Surveillance Program. See U.S. Department of Justice, Legal Authorities Supporting the Activities of the National Security Agency Described By the President (Jan. 19, 2006), *available at*

<http://www.usdoj.gov/opa/whitepaperonnsalegalauthorities.pdf>.

Finally, the public filings in this case disclose other details about the program.

Negroponte testifies in his public affidavit, for example, that the NSA utilizes its “SIGINT [signals intelligence] capabilities to collect certain international communications originating or terminating in the United States where there are reasonable grounds to conclude that one party to the communication is a member or agent of al Qaeda or an affiliated terrorist organization.”

Negroponte Unclassified Decl. ¶ 12.

As a result of these official statements and publications, the existence of the Surveillance Program is not a secret, the subjects of the program are not a secret, and the general method of the program—including that it is warrantless—is not a secret. As Judge Walker pointed out in Hepting, the government has freely acknowledged that with respect to surveillance of communications content, it has “disclosed the universe of possibilities in terms of *whose* communications it monitors and *where* those communicating parties are located.” 2006 WL 2038464, at \* 19 (emphasis in original).

With regard to the third and fourth categories of information—whether plaintiffs were subject to surveillance and information contained in the Sealed Document—I summarize what has been publicly disclosed. Both the foundation Al-Haramain and one of its directors, Al-Buthi, are “specially designated global terrorists.” Plaintiffs Belew and Ghafoor are lawyers who office in the United States and who represent Al-Haramain. Al-Buthi and Sedaghaty are directors of Al-Haramain who are believed to be living overseas, and Al-Buthi is a citizen of Saudi Arabia. Al-Buthi, Sedaghaty, Belew and Ghafoor received a copy of the Sealed Document, among other individuals including a reporter at the Washington Post. As a result of receiving the document, Al-Buthi, Sedaghaty, Belew and Ghafoor know what information the Sealed Document contains,

which means they know whether or not the government has conducted electronic surveillance of communications between Al-Haramain's director or directors and Belew and Ghafoor.<sup>3</sup>

Based on this information, plaintiffs could fall within the category of entities subject to the Surveillance Program. Nevertheless, because the government has not officially confirmed or denied whether plaintiffs were subject to surveillance, even if plaintiffs know they were, this information remains secret. Furthermore, while plaintiffs know the contents of the Sealed Document, it too remains secret. As I explain in section III, the government did not waive its state secrets privilege by its inadvertent disclosure of the document.

As for the first category of information, because plaintiffs concede that the al Qaeda threat is irrelevant to their case, and because I decline to consider at this time whether that information is necessary for the government to defend itself (see section II.B.), I decline to determine at this point whether the information is secret.

In summary, as a result of official statements and publications, general information about the Surveillance Program is not a secret. Additionally, while it is not a secret to plaintiffs whether their communications have been intercepted as may be disclosed in the Sealed Document, the government has made no official statement confirming or denying this information and it remains a secret. Finally, I have made no findings about whether specific information about the al Qaeda threat is a secret.

---

<sup>3</sup>I make this conclusion based on plaintiff's allegations and not based on the contents of the Sealed Document.

D. Whether Disclosing the Information Would Cause Harm to the National Security

Despite the fact that it is not a secret to plaintiffs whether their communications have been intercepted, the government has not confirmed or denied whether plaintiffs have been subject to surveillance, and it claims that to do so would be to disclose matters which should not be divulged due to national security concerns. The government gives several reasons for its conclusion.

The government argues that confirmation or denial of its surveillance of a particular individual might lead that individual to change his pattern of behavior, jeopardizing the ability to collect intelligence information. Negroponte Unclassified Decl. ¶ 13. This rationale does not apply to the Sealed Document; the government already inadvertently disclosed the Sealed Document to plaintiffs, thus alerting the individuals or organizations mentioned in the document that their communications have been intercepted in the past. Even if plaintiffs are not identified in the document, if they engaged in electronic communications during the period of time described in the document, and discussed the subjects identified in the document, they also know whether their communications have been intercepted. Those individuals can be presumed to have already changed their behavior as a result of any information they learned from reading the Sealed Document.

In addition, the government argues that the NSA cannot publicly confirm or deny whether any individual is subject to surveillance because to do so would tend to reveal information, sources and methods. Again, at least as to the information contained in the Sealed Document, this rationale is irrelevant. Any information, sources or methods disclosed in the Sealed Document has also been revealed to plaintiffs. In addition, plaintiffs claim that this information

is irrelevant to their case and will not need to be disclosed to the public, thereby avoiding further disclosure of any state secrets.

Finally, the government contends that even confirming or denying whether an individual has *not* been subject to surveillance would be harmful to national security. “If the NSA denied allegations about intelligence targets in cases where such allegations were false, but remained silent in cases where the allegations were accurate, it would tend to reveal that the individuals in the latter cases were targets.” Alexander Unclassified Decl. ¶ 9. This is a valid point, but plaintiffs already know whether their communications have been intercepted, and can argue *in camera*,<sup>4</sup> based on what they believe the Sealed Document reveals, that they were targets. If the Sealed Document does not reflect that plaintiffs were targets, confirming this point says nothing about plaintiffs’ target-status generally.

As I have explained, in these particular circumstances, where plaintiffs know whether their communications have been intercepted, no harm to the national security would occur if plaintiffs are able to prove the general point that they were subject to surveillance as revealed in the Sealed Document, without publicly disclosing any other information contained in the Sealed Document.

However, plaintiffs do not know whether or not their communications were intercepted beyond any that may be identified in the Sealed Document, and they do not know whether their communications continue to be intercepted. The government’s rationale for wanting to maintain the secrecy of other surveillance events rings true where plaintiffs do not know whether or not their communications have been intercepted. I am convinced that, based on the record as it

---

<sup>4</sup>I explain the use of *in camera* affidavits in Section III below.

stands now, forcing the government to confirm or deny whether plaintiffs' communications have been or continue to be intercepted, other than any communications contained in the Sealed Document, would create a reasonable danger that national security would be harmed by the disclosure of state secrets. More details about when, and whose, communications were intercepted, would allow greater insight into the methods used in the Surveillance Program, which might jeopardize the success of the Program if it is legal.

Based on the above, I have determined there is no reasonable danger that the national security would be harmed if it is confirmed or denied that plaintiffs were subject to surveillance, but only as to the surveillance event or events disclosed in the Sealed Document, and without publicly disclosing any other information in the Sealed Document. I have also concluded that disclosing whether plaintiffs were subject to any other surveillance efforts could harm the national security.

II. Government's Motion to Dismiss or in the Alternative for Summary Judgment

\_\_\_\_\_ A. Whether State Secrets are the "Very Subject Matter of the Action"

The government argues that the Surveillance Program is the very subject matter of plaintiffs' action because, it argues, plaintiffs' goal in the litigation is to determine whether the NSA has undertaken warrantless surveillance of them and, if so, whether that action was lawful. The government asserts that litigating these matters will necessarily require and risk the disclosure of state secrets. The government principally relies on Fitzgerald, 776 F.2d 1236, Kasza, 133 F.3d 1159, and El-Masri, 437 F. Supp. 2d 530.

Plaintiffs respond that the President and other Executive Branch officials have acknowledged the existence of the Surveillance Program, and that the inadvertent production of the Sealed Document makes the program no longer a secret as applied to plaintiffs.

In Fitzgerald, plaintiff claimed published statements about his purported sale of top secret marine mammal weapons systems to other countries was libelous. The court held, “Due to the nature of the question presented in this action and the proof required by the parties to establish or refute the claim, the very subject of this litigation is itself a state secret.” Fitzgerald, 776 F.2d at 1243. Nevertheless, it was only after the court determined that “there was simply no way this particular case could be tried without compromising sensitive military secrets,” that the case was dismissed. Id. The court warned that “[o]nly when no amount of effort and care on the part of the court and the parties will safeguard privileged material is dismissal warranted.” Id. at 1244.

In Kasza, former employees at a classified United States Air Force facility claimed violations of the Resource Conservation and Recovery Act (“RCRA”). The Secretary of the Air Force declared that the privilege was necessary to protect ten categories of classified information, including scientific and technological matters, physical characteristics, and environmental data. As a result, plaintiffs could not establish their *prima facie* case and, additionally, “any further proceeding in this matter would jeopardize national security.” Kasza, 133 F.3d at 1170.

Finally, El-Masri involved claims arising from plaintiff’s alleged detention pursuant to the Central Intelligence Agency’s “extraordinary rendition” program. Despite the fact that the government had confirmed the existence of a rendition program, it had offered no details about “the means and methods employed in these renditions, or the persons, companies or governments involved”—facts put directly at issue by plaintiff’s case. El-Masri, 437 F. Supp. 2d at 537. As a

result, “the whole object of the suit and of the discovery is to establish a fact that is a state secret.” Id. at 539.

In contrast to these cases, the purpose of plaintiffs’ suit is not to “establish a fact that is a state secret.” See id. The government has lifted the veil of secrecy on the existence of the Surveillance Program and plaintiffs only seek to establish whether interception of their communications—an interception they purport to know about—was unlawful. As I explained above, if plaintiffs are able to prove what they allege—that the Sealed Document demonstrates they were under surveillance—no state secrets that would harm national security would be disclosed. Accordingly, while this Court may eventually terminate some or all of plaintiffs’ claims, this case should not be dismissed outright because the very subject matter of the case is not a state secret.

\_\_\_\_\_B. Whether Plaintiffs are Unable to Demonstrate Standing or to State a Prima Facie Case, or the Government is Unable to Defend Without Privileged Information

The government argues that because of the state secrets at issue in this case, plaintiffs must be denied access to the Sealed Document or any further discovery, and, as a result, plaintiffs cannot prove standing or make out a *prima facie* case on their claims. The government, relying on the “mosaic” theory described in Halkin, asserts that *any* disclosure of *any* information related to the Surveillance Program or the Sealed Document would tend to allow enemies to discern, and therefore avoid, the means by which surveillance takes place under the program. see 598 F.2d at 8. Accordingly, the government argues, plaintiffs’ claims must be dismissed.

The government also points to the Halkin case for the principle that a number of inferences flow from the confirmation or denial of a particular individual’s international communications, including that the individual would know what circuits were used and that

foreign organizations who communicated with the targeted individuals would know what circuits were monitored and what methods of acquisition were employed. The government contends that Halkin recognized the need to protect against disclosure of information that would confirm or deny alleged surveillance, in part because it might tend to reveal other sensitive, classified information.

Plaintiffs dismiss this argument, scoffing at the mosaic theory in the context of this case where the government has already disclosed information that would trigger the Halkin concerns to the surveilled parties, albeit inadvertently. Plaintiffs also argue that the government's justification for the assertion of privilege based on possible disclosure of the nature and severity of the al Qaeda threat and the means and methods of surveillance are inapplicable to this case. They argue that no secret information regarding these issues will need to be addressed in this case, and that the merits issues are purely legal: whether there was an intentional violation of FISA, and whether the 2001 Authorization for Use of Military Force or the President's constitutional power trump FISA. Plaintiffs point out that the government presented these legal arguments already in a January 2006 white paper explaining its legal theories in support of the Surveillance Program, without revealing state secrets.

I decline to decide at this time whether this case should be dismissed on the ground that the government's state secrets assertion will preclude evidence necessary for plaintiffs to establish standing or make a *prima facie* case, or for the government to assert a defense. I recognize that disclosing information regarding the al Qaeda threat or disclosing non-public details of the Surveillance Program may harm national security, but I am not yet convinced that this information is relevant to the case and will need to be revealed.

In addition, based on my ruling that plaintiffs know from the Sealed Document whether their communications were intercepted, plaintiffs should have an opportunity to establish standing and make a *prima facie* case, even if they must do so *in camera*. Since plaintiffs already know a few pieces of the mosaic, I am unable to accept the theory that the release of *any* facts related to the Surveillance Program as applied to these plaintiffs will jeopardize national security. Contrary to Halkin, in which the plaintiffs only had proof that their names *may* have been on a watchlist and as a result their communications *may* have been acquired, plaintiffs here purport to have evidence that their communications were intercepted. See 598 F.2d at 10-11. Indeed, even the government concedes that “Plaintiffs remain free to make any allegations and assert any arguments in support of their standing, or any other argument, as they deem appropriate, and the Court has the power to review the sealed classified document in order to assess Plaintiffs’ claims and arguments.” Reply in Supp. of Defs.’ Mot. to Prevent Pls.’ Access to the Sealed Classified Document at 19.

Nevertheless, I may conclude, after exploring the procedures described in section VII below, that there is no way plaintiffs can prove their case without compromising state secrets, or no possibility that the government can properly defend the allegations.<sup>5</sup> I recognize that the government believes any further proceedings in this case would be futile, but I am just not

---

<sup>5</sup>I note, for example, the fact that the government has claimed the state secrets privilege, in addition to statutory privileges, in answer to plaintiffs’ interrogatory requesting information about whether a warrant was obtained. Plaintiffs indicated in oral argument that they would rely on public statements and statements in the Sealed Document to prove the surveillance was warrantless. If after holding the discovery conference discussed in section V, I uphold the government’s invocation of the privilege, plaintiffs will have to proceed based on what is publicly disclosed and what they are able to argue *in camera* that the Sealed Document discloses. Simply put, plaintiffs should have an opportunity to make that argument.

prepared to dismiss this case without first examining all available options and allowing plaintiffs their constitutional right to seek relief in this Court. See Spock v. United States, 464 F. Supp. 510, 519 (S.D.N.Y. 1978) (“[a]n aggrieved party should not lightly be deprived of the constitutional right to petition the courts for relief”).

C. Dismissal Based on Statutory Privileges

The government argues that two statutory privileges also protect the intelligence-related information, sources and methods in this case, requiring the dismissal of the action. It claims that Section 6 of the National Security Act, 50 U.S.C. § 402 prohibits disclosure of any information in this case. That section provides that “nothing in this Act or any other law . . . shall be construed to require the disclosure of the organization or any function of the National Security Agency, of any information with respect to the activities thereof . . .” 50 U.S.C. § 402. The government makes the same claim for Section 102A(i)(1) of the Intelligence Reform and Terrorism Prevention Act of 2004, 50 U.S.C. § 403-1(i)(1), which requires the Director of National Intelligence to protect intelligence sources and methods from unauthorized disclosure.

Plaintiffs argue that neither statutory privilege applies because they are co-extensive with the state secrets privilege, and because plaintiffs’ claims can be litigated on the merits without any need to know defendants’ secret sources and methods. Plaintiffs point out that none of the cases cited by the government involved the dismissal of a case based on the assertion of one of the statutory privileges.

The statutory privileges at issue here do not direct the dismissal of this action, nor am I yet convinced that they will block evidence necessary to plaintiffs’ case. Plaintiffs should have an opportunity to attempt to show standing and a *prima facie* case based on what is currently

available to them and any evidence that I have determined is not covered by the state secrets privilege. In proceeding with the discovery process, the government is free to identify discovery requests that fall within these other statutory privileges, and explain specifically why this is so, and I will determine whether the privileges prevent plaintiffs from discovering that specific evidence.

Based on the analysis above, I deny the government's motion to dismiss. I also deny the government's motion for summary judgment in order to allow plaintiffs to conduct discovery, but I give the government leave to renew its motion.

### III. Defendants' Motion to Deny Plaintiffs' Access to Sealed Document

The government argues in its Motion to Prevent Plaintiff's Access to the Sealed Document that the document remains classified, regardless of the inadvertent and unauthorized disclosure. See Exec. Order No. 12,958, § 1.1(b), as amended by Exec. Order No. 13,292 ("Classified information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information."). According to the government, the Executive has sole power to protect classified information. The decision to authorize or deny a security clearance lies exclusively with the Executive, and a district court cannot assess the merits of such a decision. Dormfort v. Brown, 913 F.2d 1399, 1401 (9th Cir. 1990). The government further argues that plaintiffs cannot be allowed access to the Sealed Document because such access would carry with it an unacceptable risk of unauthorized disclosure. The government also invokes the state secrets privilege over the document. Finally, the government requests that I order plaintiffs to return to the government all copies of the Sealed Document.

Plaintiffs respond that, under the doctrine of separation of powers, the court has inherent authority to allow access to documents under its control, as the Sealed Document now is. Plaintiffs also argue that if the court rules that they may have access to the Sealed Document, such a decision is subject to judicial immunity. Furthermore, plaintiffs assert that the court has the authority to ensure that the decision to classify a document was not made for the purpose of concealing unlawful conduct, citing cases in which courts have conducted *de novo* review of the classified status of documents.

Plaintiffs correctly point out that the Supreme Court has recognized that district courts have “the latitude to control any discovery process which may be instituted so as to balance respondent’s need for access to proof which would support a colorable constitutional claim against the extraordinary needs of the CIA for confidentiality and the protection of its methods, sources, and mission.” Webster v. Doe, 486 U.S. 592, 604 (1988). Plaintiffs then contend that because defense counsel have access to the Sealed Document, due process requires that plaintiffs’ counsel have access as well.

I accept the government’s argument that the inadvertent disclosure of the Sealed Document does not declassify it or waive the state secrets privilege. In addition, I am unwilling to use any “inherent authority” of the Court to give plaintiffs access to the document, and I decline at this time to accept plaintiffs’ invitation to overrule any classification decision made by the government as to the entire document. The cases plaintiffs rely on in support of their demand that I review *de novo* the reasons for the classification of the Sealed Document caution that courts are to proceed very carefully in reviewing classification decisions and should not “second-guess” classification decisions when the “judiciary lacks the requisite expertise.” See McGehee

v. Casey, 718 F.2d 1137, 1149 (D.C. Cir. 1983); American Library Ass'n v. Faurer, 631 F. Supp. 416, 423 (D.D.C. 1986) (citing McGehee); ACLU v. Dep't of Defense, 389 F. Supp. 2d 547, 564 (S.D.N.Y. 2005) (within CIA's ken to evaluate the risks of disclosure to intelligence-gathering); Salisbury v. United States, 690 F.2d 966, 970 (D.C. Cir. 1982) ("accord substantial weight" to classification decision).

The Executive has not granted authority to plaintiffs to review classified materials, and the document remains classified. In addition, if plaintiffs were given full access to the document, plaintiffs may refer back to it and reflect on what it does or does not disclose. For example, they may confirm which modes of communication were vulnerable to interception and avoid those modes. The government has raised sufficient grounds for concern and I grant the government's motion.

At the same time, since the government expressly concedes that "the Court has the power to review the sealed classified document in order to assess Plaintiffs' claims and arguments," I will permit plaintiffs to file *in camera* any affidavits attesting to the contents of the document from their memories to support their standing in this case and to make a *prima facie* case. See Reply in Supp. of Defs.' Mot. to Prevent Pls.' Access to the Sealed Classified Document at 19. The government may request that these declarations be deposited in the SCIF.

In addition, I urge the government to consider again whether redactions to the document may be undertaken given my ruling that it is no longer a secret to plaintiffs as to what information the Sealed Document contains. For example, perhaps some of the information in the Sealed Document should be shared with plaintiffs, subject to a protective order, as it is now innocuous, such as the fact of this particular surveillance event, and any dates contained in the

document. If it is possible to disentangle those details from whatever else the Sealed Document may reveal about the Surveillance Program more generally, and if this information is necessary to plaintiffs' case, I may want to attempt such an exercise.

Therefore, I grant the government's Motion to Deny Plaintiffs' Access to the Sealed Document in that plaintiffs may not have physical control over the entire document. Plaintiffs may, however, submit affidavits *in camera* to support their standing and to make a *prima facie* case. After exploring possible redactions, I may require that plaintiffs be provided with information that is now no longer "secret," subject to a protective order.

Finally, pursuant to the government's request, I order plaintiffs to deliver to my chambers all copies of the Sealed Document in their possession or under their control.<sup>6</sup> I will contact the government upon receipt of any copies, at which time the government may collect the copies and deposit them in the SCIF.

#### IV. Whether FISA Preempts the State Secrets Privilege

Plaintiffs argue in their opposition both to the government's motion to dismiss and the motion to deny access to the Sealed Document that FISA preempts the state secrets privilege. Specifically, plaintiffs argue that FISA vests the courts with control over materials relating to electronic surveillance, subject to "appropriate security procedures and protective orders." 50 U.S.C. § 1806(f). As a result, plaintiffs contend that Section 1806(f) renders the state secrets privilege superfluous in FISA litigation.

---

<sup>6</sup>I note that both Belew and Ghafoor have testified via declaration that they complied fully with the FBI's request to destroy or return all copies of the Sealed Document.

The government responds that Section 1806(f) is inapplicable to this case, because the provision was enacted for the benefit of the government. The government argues that Section 1806(f) authorizes district courts, at the request of the government, to review *in camera* and protect classified information when the government intends to use evidence *against* an individual. Indeed, the government contends, the statute and the case law demonstrate that the “aggrieved person” language is “someone as to whom FISA surveillance has been made known, typically in a criminal proceeding.” Defs.’ Reply in Supp. of Mot. to Dismiss/Summ. J. at 18. In this case, it argues, where the threshold question of whether or not plaintiffs have been subject to surveillance is itself a state secret, plaintiffs cannot use FISA to confirm their belief. In addition, the government argues, there is no clear congressional statement to overturn the privilege.

The relevant inquiry in deciding whether a statute preempts a federal common law privilege<sup>7</sup> is whether the statute speaks directly to the question otherwise answered by federal common law. Kasza, 133 F.3d at 1167. There is a presumption in favor of the privilege “except when a statutory purpose to the contrary is evident.” Id.

The language of § 1806(f) is broad, providing, in relevant part:

Whenever a court . . . is notified pursuant to subsection (c) or (d) of this section [describing occasions when the government intends to use information obtained through surveillance], or whenever a motion is made pursuant to subsection (e) [motion to suppress], or whenever any motion or request is made by an aggrieved person pursuant to any other statute or rule of the United States . . . to discover or obtain applications or orders or other materials relating to

---

<sup>7</sup>The government argues that the state secrets privilege is also constitutionally-based, deriving from the President’s “most basic constitutional duty” to protect the Nation from armed attack, and suggests a different method of evaluating whether FISA preempts the state secrets privilege. Specifically, according to the government, Congress must set forth a “clear statement” that it intended to intrude on powers of the Executive. United States v. Bass, 404 U.S. 336, 350 (1971).

**electronic surveillance** or to discover, obtain, or suppress evidence or information obtained or derived from electronic surveillance under this chapter, the United States district court . . . shall, notwithstanding any other law, if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would **harm the national security of the United States**, review in camera and ex parte the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted.

50 U.S.C. § 1806(f) (emphasis added). The provision goes on to state that:

In making this determination, the court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance.

Id.

“Aggrieved person” is defined by the statute to mean, “a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance.” 50 U.S.C. § 1801(k). Finally, under Section 1810, “An aggrieved person, other than a foreign power or an agent of a foreign power, . . . who has been subjected to an electronic surveillance . . . in violation of section 1809 [engages in electronic surveillance except as authorized by statute] shall have a cause of action against any person who committed such violation . . .” 50 U.S.C. § 1810.

To summarize, Section 1810 gives a private right of action to an “aggrieved person,” so long as the person is not a foreign power or an agent of a foreign power. An “aggrieved person” is someone whose communications have been subject to surveillance. Pursuant to Section 1806(f), a plaintiff, if he is able to show he is an “aggrieved person,” may seek “to discover or obtain applications or orders or other materials relating to electronic surveillance or to discover, obtain, or suppress evidence or information obtained or derived from electronic surveillance

under this chapter [FISA].” Upon an affidavit from the Attorney General that “disclosure or an adversary hearing would harm the national security of the United States,” the court may review *in camera* and *ex parte* “the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted.” To accept the government’s argument that Section 1806(f) is only applicable when the government intends to use information against a party would nullify FISA’s private remedy and would be contrary to the plain language of Section 1806(f).

The question then becomes whether Section 1806(f) preempts the state secrets privilege. I decline to reach this very difficult question at this time, which involves whether Congress preempted what the government asserts is a constitutionally-based privilege. Given that the government has already permitted the court to review the Sealed Document *in camera* and has expressly conceded that I may evaluate plaintiffs’ claims based on my review of that document, I need not resolve this question presently.

#### V. Plaintiffs’ Motion for Order Compelling Discovery

Plaintiffs’ Motion for Order Compelling Discovery seeks responses from the government to interrogatories. The interrogatories request answers to whether electronic surveillance was conducted of Al-Haramain or its director and counsel, dates of such surveillance, and whether the FISA court issued warrants for such surveillance. The interrogatories also seek information about the classification of the Sealed Document, including what date the decision to classify it as SCI was made, what officials made that decision, and the reason for that classification.

The government makes substantially the same arguments in support of its opposition to plaintiffs’ motion to compel discovery as it does in its memorandum in support of its motion to

dismiss. It argues that it has not acknowledged the specific surveillance alleged in this case, even if it has acknowledged the Surveillance Program more generally, and that it cannot respond to the interrogatories because all possible answers would be subject to the state secrets privilege.

Given my rulings that it is no longer secret to plaintiffs whether their communications were intercepted as described in the Sealed Document, and that there would be no harm to national security if plaintiffs' general allegations were confirmed or denied as to that specific circumstance, I will hold a discovery conference to determine to which interrogatories plaintiffs need answers, and to which interrogatories the government should be required to respond. I may require the government to provide specific responses to the interrogatories for *in camera, ex parte* review on an item-by-item basis as was generally approved by In re United States. See 872 F.2d at 478. Nevertheless, I will ensure that further steps in the discovery process are taken with the Supreme Court's caution in mind; the claim of privilege is accorded the "utmost deference," unless a court is not satisfied under the particular circumstances of the case that "there is a reasonable danger that compulsion of the evidence will expose military matters which, in the interest of national security, should not be divulged." Reynolds, 345 U.S. at 10.

As a result, I deny Plaintiffs' Motion for Order Compelling Discovery, with leave to renew after the discovery conference.

#### VI. Oregonian's Motion to Unseal Records

The Oregonian argues in its motion to unseal records that there is a strong presumption supporting access to court records, and that a court must state the compelling interest requiring an order to seal, "along with findings specific enough so that a reviewing court can determine whether the closure order was properly entered." Oregonian Publishing Co. v. United States

Dist. Ct. for the Dist. of Or., 920 F.2d 1462, 1464 (9<sup>th</sup> Cir. 1990). The Oregonian suggests that even if the Sealed Document is classified, sealing of the document may be inappropriate if it is possible to redact only the few lines that require confidential treatment. United States v. Ressam, 221 F. Supp. 2d 1252, 1263-64 (W.D. Wash. 2002). The newspaper argues that the Sealed Document should be unsealed because no compelling interest supports further sealing and, in any event, any interest is outweighed by the constitutional and common law rights of public access to court documents.

The government responds that the document was and remains classified as SCI and “TOP SECRET,” notwithstanding its inadvertent disclosure to the plaintiffs, and that the Executive has sole authority to classify or declassify information.<sup>8</sup> The government further asserts that before the court evaluates whether a compelling interest requires continued protection of a document, the court must first address whether the place and process have historically been open to the press and general public and whether public access plays a significant positive role in the functioning of the particular process in question. Phoenix Newspapers, Inc. v. United States Dist. Ct. for the Dist. of Arizona, 156 F.3d 940, 946 (9<sup>th</sup> Cir. 1998). Here, according to the government, the Sealed Document remains a classified document of the sort to which the press or public have historically not had access.

Given my decision above that the inadvertent disclosure of the Sealed Document does not declassify it or waive application of the state secrets privilege, I must deny the Oregonian’s

---

<sup>8</sup>On April 14, 2006, the government submitted a Classified Declaration in Opposition to Oregonian Publishing Company’s Motion to Intervene and Unseal Records, and on May 12, 2006, the government filed a Superseding Classified Declaration. I have not reviewed either of these declarations submitted *in camera* and *ex parte*.

Motion to Unseal Records. Even if the document were one to which the press or public have historically had access by virtue of its being filed with the Court, the government has asserted a compelling national security interest that overrides any public interest in the document. While I may entertain the possibility that plaintiff may have access to any innocuous information in the document based on the fact that it is no longer secret to them, and subject to a protective order, the document contains highly classified information that must not be disclosed to the public.

VII. Further Proceedings

I will schedule a discovery conference at which the parties should be prepared to discuss the following issues: possible redactions to the Sealed Document, possible stipulations, item by item review of interrogatory requests to consider whether *in camera* responses would be appropriate, depositions, hiring an expert to assist the Court in determining whether any of these disclosures may reasonably result in harm to the national security, and any other appropriate discovery issues. The parties should confer on a few mutually convenient dates and times and contact the Court to reserve a time.

VIII. Certification for Appeal

Since I recognize, as did Judge Walker in Hepting, that my rulings on the Motion to Dismiss or, in the Alternative, for Summary Judgment and Motion to Prevent Plaintiffs' Access to the Sealed Classified Document "involve[] a controlling question of law" about which there is "substantial ground for difference of opinion," and since "an immediate appeal from the order may materially advance the ultimate termination of this litigation," I certify these rulings for immediate appeal. U.S.C. § 1292(b). If the parties choose to appeal, and if the appeal is taken, the parties may move to stay proceedings in the district court.

## CONCLUSION

The government's Motion to Dismiss or, in the Alternative, for Summary Judgment (#58) is denied, but the government has leave to renew its Motion for Summary Judgment. The government's Motion to Prevent Plaintiffs' Access to the Sealed Classified Document (#39) is granted. Plaintiffs' Motion for Order Compelling Discovery (#35) is denied with leave to renew. Oregonian Publishing Company's Motion to Intervene was previously granted, but its Motion to Unseal Records (#7) is denied.

IT IS SO ORDERED.

Dated this 7th day of September, 2006.

/s/ Garr M. King  
Garr M. King  
United States District Judge